GHENT UNIVERSITY

Course Specifications

Valid in the academic year 2021-2022

Blockchain Technologies and Applications (E034150)

Due to Covid 19, the education and assessment methods may vary from the information displayed in the schedules and course details. Any changes will be communicated on Ufora.

Course size *(nominal values; actual values may depend on programme)*

Credits 3.0	**Study time 90 h**	**Contact hrs**	15.0h

Course offerings and teaching methods in academic year 2021-2022

A (semester 1)	English	Gent	microteaching	2.5h
			lecture	12.5h
			group work	1.25h

Lecturers in academic year 2021-2022

De Sutter, Bjorn	TW06	lecturer-in-charge

Offered in the following programmes in 2021-2022	**crdts**	**offering**
Master of Science in Computer Science	3	A
Master of Science in Computer Science Engineering	3	A
Master of Science in Computer Science Engineering	3	A
Master of Science in Information Engineering Technology	3	A
Exchange Programme in Computer Science (master's level)	3	A

Teaching languages

English

Keywords

blockchain, consensus management, decentralized ledgers, Bitcoin, Ethereum, smart contracts, attacks and defenses, cryptocurrencies

Position of the course

- Blockchain technology, as used for cryptocurrencies such as Bitcoin and Ethereum, but also being extended for other purposes, has the potential to facilitate the next wave of ICT innovation, following the previous waves of Internet connectivity and the Internet of Things.
- Currently, blockchain technology is a domain where practice is ahead of theory. Systems are being deployed in practice, while many fundamental questions are still open concerning privacy, scalability, and security. Despite this observation and hence the lack, to some extent, of theoretic foundations and models, it is important that graduating students know the core technology and concepts, and their potential.
- Blockchain technology relates to cryptography (as cryptographic primitives are used extensively to secure the blockchains), to distributed computing (as a blockchain is a distributed ledger and blocks are added to the chain and validated in a distributed manner), and computer security, as it inherently evolves around building trust among untrusting partners.
- A course focused on the fundamental concepts technologies underlying blockchains, and on the applications thereof can hence complement the existing courses on information security, parallel and distributed programming and computing, and software hacking and protection.

Contents

- General introduction, including
  - core concepts: byzantine fault tolerance - generals problem, public decentralized transaction ledgers, proof-of-work, proof-of-stake, proof-of-space, immutability, honest majority, hash functions, Merkle trees, transactions, blocks, blockchain, roles and separation of consensus

management and digital asset management;
  - types of blockchains: permissionless vs. permissioned ledgers;
  - distributed consensus mechanisms;
  - transparency, censorship, anonymity, pseudonimity, unlinkability, zero-knowledge proofs.
- Bitcoin: Nakamoto consensus, miners, wallets, addresses & other data structures, hash puzzles, longest chain rule, concrete implementation & algorithms, double spending attacks & mitigation, consensus management, network & communication management, gossiping protocol, pooled mining, coin management tools, user experience and security, pseudomynous vs. anonymous
- Alternative blockchain technologies and consortiums, permissioned ledger, regulatory requirements, access control
- Data in blockchains: trusted parties, interplanetary database, data validation by means of oracles,
- Ethereum: smart contracts, Ethereum Virtual Machine, security issues of smart contracts, programming languages for smart contracts
- Mining alternatives: clouds, processor & accelerator architectures, performance and energy consumption, scalability, sustainability, trusted software (running in enclaves), proof-of-elapsed time, proof-of-useful-work
- Applications in various domains: energy markets, property titles and other public services, medical records, academic transcripts, airlines - passenger - flight management, IoT, financial products, insurance, production chains, media and entertainment;

Initial competences

- It is expected that the contents of the course on Computer Architecture are well understood.
- A basic understanding of data structures, programming languages, computer networks, and operating systems is expected.

Final competences

1 Deep understanding of underlying concepts, problems solved, applications, and open issues of blockchains.
2 Understanding technological foundations of blockchains.
3 Overview of alternative technologies for basic components of blockchains.
4 Deep understanding of potential security issues, attacks, and defenses.
5 Understanding potential of blockchains to disrupt industries and to drive new applications and business models.
6 Differentiate scenarios that cannot benefit from blockchain technology (against the hype) from those that can.

Conditions for credit contract

Access to this course unit via a credit contract is determined after successful competences assessment

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Group work, Microteaching, Lecture

Extra information on the teaching methods

- Core material will be presented in lectures by the lecturer. If the number of students that wants to attend the lectures fits in the assigned room, lectures will be on campus. Otherwise, they will be live online.
- In small groups, students will study current use cases, best practices, and advanced technical aspects of block chains and present that to each other as microteaching. The lecturer advises them during the studying and the preparation of the presentation.
- On Ufora, the students are given small assignments for which they have to consult sources of information on their own.

Learning materials and price

- Lecture slides (free)
- Additional notes & papers at copying cost

References

- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven

Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.
- A myriad of online sources.

Course content-related study coaching

- Online discussion forum
- Feedback on online assignments and Q&A about them in next lecture.
- Contact via chat, mail and an open door policy.
- Question time before and after each lecture.
- Lecturer advises student group work in preparation of microteaching, meeting multiple times to discuss their progress.

Assessment moments

end-of-term and continuous assessment

Examination methods in case of periodic assessment during the first examination period

Written examination with open questions

Examination methods in case of periodic assessment during the second examination period

Written examination with open questions

Examination methods in case of permanent assessment

Oral examination, Peer assessment

Possibilities of retake in case of permanent assessment

examination during the second examination period is possible in modified form

Extra information on the examination methods

Permanent evaluation: peer assessment, oral examination: student presentations
For the permanent evaluation, the peer presentation of the student on a current, assigned topic will be graded. Both the student's general presentation skills and the contents of the presentation will be graded. Peer assessment will be used as additional input for the examiner to determine the mark.

Calculation of the examination mark

The permanent evaluation determines 1/5 of the total mark. Students can only pass the course if they achieve at least 10/20 for the permanent evaluation and 10/20 for the end-of-term exam. In case this requirement is not met, but the computed weighted score is 10/20 or more, the final score is reduced to 9/20.

Facilities for Working Students

Option to be freed from presence in labs with alternative assignment after consultation with the responsible teacher. Option for oral exam with written preparation at another time in the academic year. Option for feedback by appointment during and after business hours.